区块链技术深度剖析

主 讲 人：bjgpdn

邮　　件：wbaocheng@ncut.edu.cn

技术支持：北京亚鼎智能科技有限公司
大连泰尔科技有限公司

关于本课程

课程性质与学习目标

- 网络空间安全（信息安全）专业兴趣选修课。
- 理解和掌握区块链、密码技术、共识机制、激励机制、智能合约、P2P网络等基本原理和实践应用。
- 掌握比特币源码（版本：0.1.5）及典型密码算法的实践应用。
- 领会区块链中安全机制的设计思想、区块链未来的应用价值和发展趋势。
- 加强“区块链思维”训练，学会设计行业应用方案。

关于本课程

教学用书

- 教材
  - 自编或网络资料
- 参考书
  - 邹均, 曹寅，刘天喜等. 区块链技术指南，机械工业出版社，2016.
  - 申屠青春. 区块链开发指南，机械工业出版社，2017.
  - ……

关于本课程

课程重点和难点

- 重点
  - 区块链原理理解和掌握
  - 密码算法思想和原理的掌握
  - 比特币源码以及第三方密码库的使用
- 难点
  - 用密码学思想分析区块链原理并且编程实现

关于本课程

考核方式

总成绩的分配

期末总成绩	实践成绩	平时成绩(30分)		
		作业	考勤	学风
100分	70	10	10	10

1、“考勤”成绩指上课迟到或不到情况的考核

2、“学风”成绩指课堂纪律和作业独立完成的考核

第一讲 区块链概述

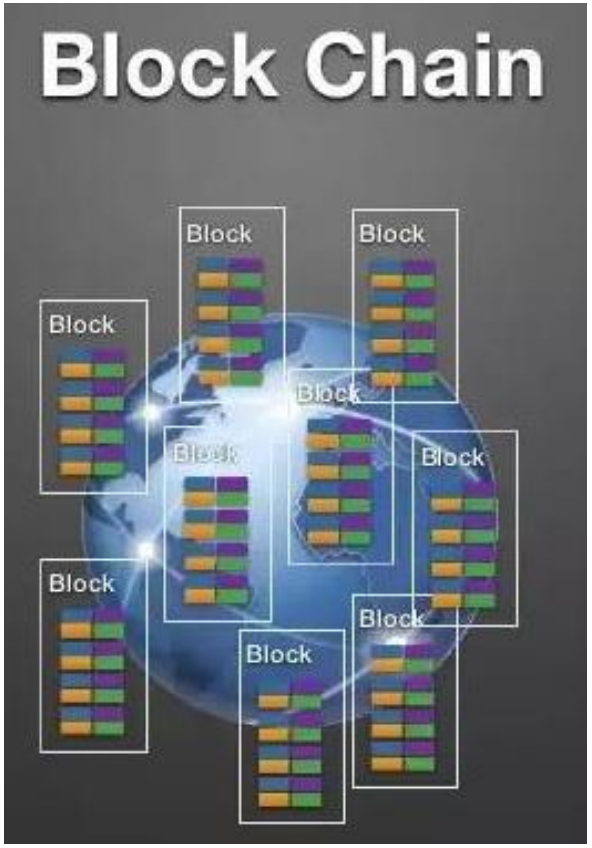
本讲主要内容

- 构建诚信社会
- 区块链与密码学
- 区块链技术原理

第一讲 区块链概述

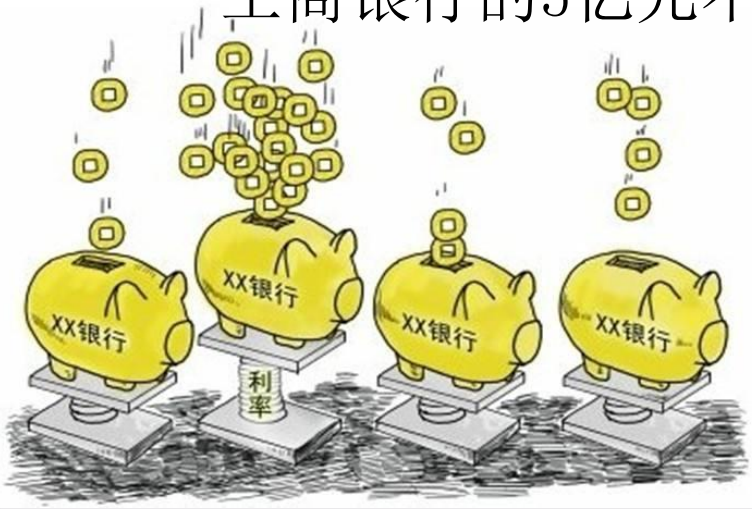
本讲主要内容

- 构建诚信社会
- 区块链与密码学
- 区块链技术原理



问题1 - 银行存款凭空消失，能找回吗？谁来负责？

- 2015年，我国多地频频出现银行储户存款“失踪”案件：浙江杭州42位银行储户发现，自己的数百万元存款仅剩少许甚至被“清零”；泸州老窖等知名企业存款也出现“异常”，甚至还出现3个月内农业银行、工商银行的5亿元不知去向。



问题2 - 陌生人之间如何实现相互信任？

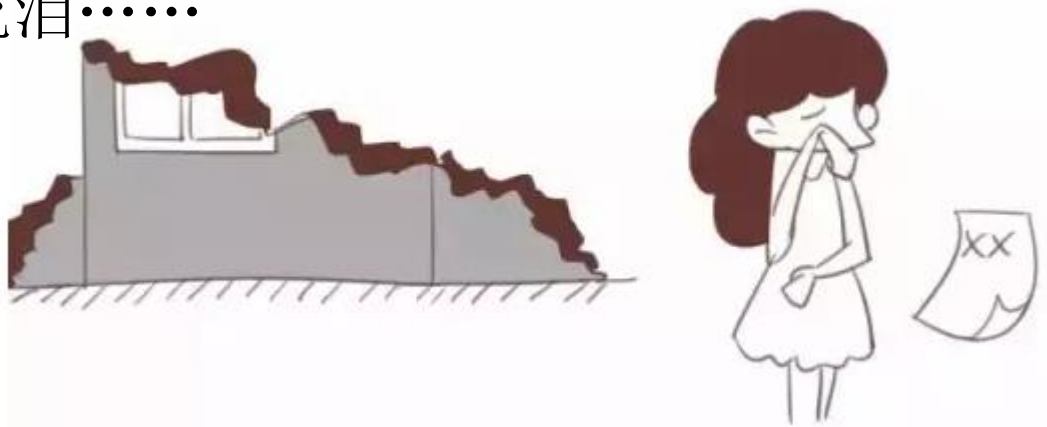
- 北京的小赵想租个房子，房东告诉小赵他的房子不但新，而且各种设施完善，家具出了问题他都可以免费更换，租金还便宜。这么好的事，小赵肯定要掂量掂量：这房东是不是在唬我？

问题2 - 陌生人之间如何实现相互信任？

- 同样的，小赵还想买辆二手车，但是卖家会有动机虚报自己的里程数，甚至谎称自己的车子没有经历过事故和维修，小赵该如何判断呢？

问题3 - 已发生的交易记录如何不被篡改？

- 玛丽安娜女士居住在洪都拉斯，她住在自家房子三十多年了。某天，玛丽安娜遭到法院传讯。A向法院申请驱逐令，原来国家产权局登记的是A的名字，而后房屋被拆毁。但后来经过法院查证，房子其实就是人家玛丽安娜女士的，但不动产已经毁了，玛丽安娜女士只能默默流泪……



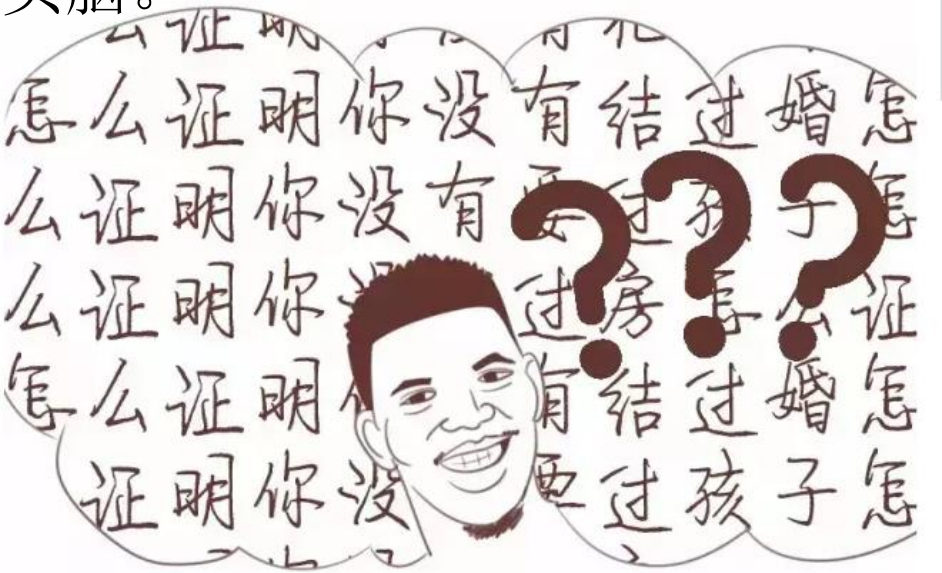
问题4 - 该怎么证明我妈是我妈？如何实现自证？

- 北京市民陈先生一家三口准备出境旅游，需要明确一位亲人为紧急联络人，于是他想到了自己的母亲。可问题来了，需要书面证明他和他母亲是母子关系。可陈先生在北京的户口簿，只显示自己和老婆孩子的信息，而父母在江西老家的户口簿，早就没有了陈先生的信息。

- 陈先生如何证明我妈是我妈呢？

问题4 - 该怎么证明我妈是我妈？如何实现自证？

- 同样的情况还有要证明你没犯过罪，要证明你没结过婚，要证明你没有要过孩子，要证明你没买过房……这样那样的证明，有的听起来莫名其妙，办起来更让人东奔西跑还摸不着头脑。



1.0 构建诚信社会 - 引言

- 当前，社会诚信缺失问题非常突出，各种假冒伪劣、坑蒙拐骗、弄虚作假、尔虞我诈现象，给我国经济社会生活带来了无法估量的信任危机。
- 诚信缺失已经成为制约我国市场经济高效快速发展和社会文明建设的一个重要因素。
- 因此，我们必须正视我国诚信缺失的现状，深刻认识其危害性，把握现代社会中诚信缺失的社会原因，寻找解决方案，为治理诚信缺失问题提供有效的策略。

1.1 构建诚信社会 - 公信力

- 现实社会中，人与人、人与公司、公司与公司之间的交易需要公信力提供支撑。
- 公信力一般由政府、国家机关或政府授权的第三方组织提供。通俗来说，公信力就是使公众信任的力量。
- 银行存款“失踪”、e租宝诈骗—利用公信力为高风险的互联网金融产品进行背书，是否会对政府以及媒体的公信力带来损害？
- 用技术解决公信力—区块链（Blockchain）

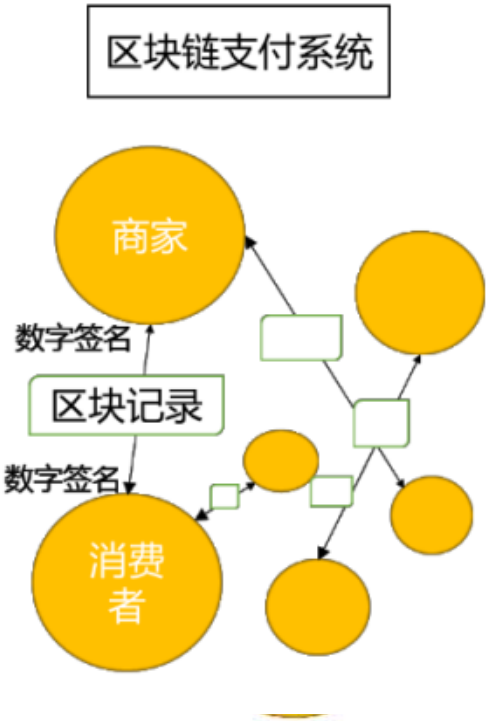
1.2 构建诚信社会 - 区块链

- 区块链技术的核心功能指在提升公信力。
- 当前公信力模型中公信力仅由政府或政府所授权的第三方机构掌握，政府的自我监督能力未必能够被社会充分认可。
- 区块链技术可以很好地满足公信力需求，并把公信力抽象出来作为一个“去中心化”的存在，形成政府、大众、区块链与公信力互相监督的“公信新格局”。
- 即信任是建立在区块链上的，而非由单个组织掌控，公信力可以被多方交叉验证与监督，得以实现和保障。

1.3 构建诚信社会 - 什么是区块链 - 背景

- 互联网上的贸易，几乎都需要借助可资信赖的第三方信用机构来处理电子支付信息。这类系统仍然内生性地受制于“基于信用的模式”。

- 区块链技术是构建比特币区块链网络与交易信息加密传输的基础技术。它基于密码学原理而不基于信用，可使得任何达成一致的双方直接支付，从而不需要第三方中介的参与。



1.3 构建诚信社会 - 什么是区块链 - 定义

- 区块链是一个分布式账本，一种通过去中心化、去信任的方式集体维护一个可靠数据库的技术方案。
- 从数据角度来看：区块链是一种几乎不可能被更改的分布式数据库。这里的“分布式”不仅体现为数据的分布式存储，也体现为数据的分布式记录（即由系统参与者共同维护）。
- 从技术的角度来看：区块链并不是一种单一的技术，而是融合了多种技术的一个集成式创新。这些技术以新的结构组合在一起，形成了一种新的数据记录、存储和表达的方式。

1.3 构建诚信社会 - 什么是区块链 - 特征

- 开放、共识
  - 任何人都可以参与到区块链网络，每一台设备都能作为一个节点，每个节点都允许获得一份完整的数据库拷贝。节点间基于一套共识机制，通过竞争计算共同维护整个区块链。任一节点失效，其余节点仍能正常工作。
- 去中心、去信任
  - 区块链由众多节点共同组成一个端到端的网络，不存在中心化的设备和管理机构。节点之间数据交换通过数字签名技术进行验证，无需互相信任，只要按照系统既定的规则进行，节点之间不能也无法欺骗其它节点。

1.3 构建诚信社会 - 什么是区块链 - 特征

- 交易透明、双方匿名
  - 区块链的运行规则是公开透明的，所有的数据信息也是公开的，因此每一笔交易都对所有节点可见。由于节点与节点之间是去信任的，因此节点之间无需公开身份，每个参与的节点都是匿名的。
- 不可篡改，可追溯
  - 单个甚至多个节点对数据库的修改无法影响其他节点的数据库，除非能控制整个网络中超过51%的节点同时修改，这几乎不可能发生。区块链中的每一笔交易都通过密码学方法与相邻两个区块串联，因此可以追溯到任何一笔交易的前世今生。

1.4 构建诚信社会 - 什么是区块链 - 政府支持

- 2016年1月，英国发表区块链白皮书，明确指出：区块链列入英国国家战略部署。
- 2016年10月18日，工信部发布《中国区块链技术和应用发展白皮书》。
- 2016年12月，国务院将区块链写入《“十三五”国家信息化规划》，与大数据、人工智能等成为国家战略前沿技术。
- 2017年5月16日，工信部发布首个区块链标准《区块链参考架构》。
- 国务院2017.10.13印发《关于积极推进供应链创新与应用的指导意见》：提高质量安全追溯能力。

1.4 构建诚信社会 - 什么是区块链 - 国内外动态

- 国际权威杂志《经济学人》、《哈佛商业周刊》、《福布斯杂志》等相继报道区块链技术将影响世界。
- 创业公司R3联合全球42家顶级银行成立区块链联盟，包括摩根大通、美国银行、汇丰银行、花旗银行、富国银行、三菱UFJ金融集团、巴克莱银行、高盛、德意志银行等。
- 百度加入Linux基金会领导的超级账本（Hyperledger）区块链联盟，成为该联盟最新成员。
- 金融区块链合作联盟深圳成立，腾讯华为加入。
- 腾讯发布区块链方案白皮书……

1.5 该怎么证明我妈是我妈？如何实现自证？

- 2008年，区块链(Blockchain)的概念浮出水面。
- 该技术将数据分区块存储，每一块包含一部分内容
- 每一个区块都会记录着前一区块的ID（唯一标识）
- 按时间顺序形成一个链状结构，并以密码学方式保证数据不可篡改，因而称为区块链技术。

1.6 区块链 - 未来已来，只是尚未流行

- 想象一下：一个人从小学开始，每一年的成绩单，每一个学校的毕业证都可以在区块链上查到。
- 工作状况、婚姻状况、保险状况也都一一呈现在区块链之上。医生的每一次诊断都将写入区块不可修改。
- 数字仲裁可以直接从区块链上扣款，公益捐款的每一笔收和用途都记录在案。
- 我们生活的社会将不仅是一个数字化社会，而是区块链所带来的诚信社会。
- 未来已来，只是尚未流行，我辈仍需多努力……

北方工业大学

Q&A

第一讲 区块链概述

本讲主要内容

- ✓ 构建诚信社会
- ➢ 区块链与密码学
- ◆ 区块链技术原理

2.1 引言

- 区块链：一座类似“94年互联网”的金矿，方兴未艾
  - 国内外金融巨头投身区块链技术的应用和研发
  - IBM、微软等主流技术公司也全面介入
  - 区块链领域的投资更是呈现出爆发式增长

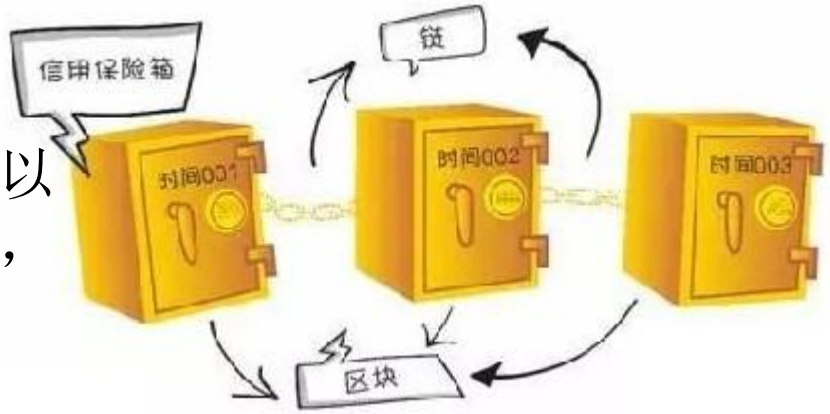
- 2016：“区块链元年”；2017：“区块链战略元年”
- 尴尬现状——概念上大火，实践仍停留在起步阶段

2.1 引言

- 繁华落尽， 2017，将洗尽铅华，从浮躁中抬起头来
- 区块链技术是金融科技的核心，还被认为是继PC、互联网、社交网络、智能手机之后，人类的第五次计算革命，是下一代价值互联网的基石，为人类社会进入透明、可靠的信用社会打开了大门。
- 马云曾经说过：“很多人还没有搞清楚什么是PC互联网，移动互联网来了，我们还没有搞清楚移动互联的时候，大数据时代又来了”——区块链又来……
- 区块链技术将改变世界！我们正站在风口上……

2.2 区块链与密码学

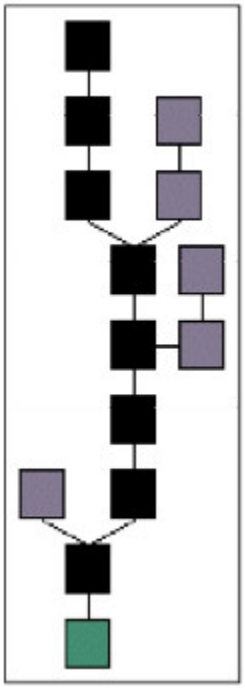
- 区块链是比特币的底层技术，可应用于其它不同领域
- 区块链创造了一个“信任机制”，部署在点对点网络中，以密码学为基础，以共识机制为纲要，用一种链式结构存放数据。
  - 在比特币网络中，数据以文件的形式被永久记录，这些记录称之为区块。



- 特点：分布式（去中心化）、匿名性（无需信任）、开放性（高度透明）、加密安全性（不可篡改）。

2.2 区块链与密码学

- 区块链是由一串使用密码学方法产生的、从后向前按时间有序链接起来的数据区块（包含若干交易信息）组成的数据结构。
  - 每个区块都包含了前一区块（父区块）的哈希值(hash)；
  - 区块通过“父区块哈希值”字段引用（指向）父区块；
  - 把每个区块链接到各自父区块的哈希值序列就创建了一条一直可以追溯到第一个区块（创世区块）的链条。



2.2 区块链与密码学 - 什么是密码学？

- 密码学是用来保证信息安全的一种必要的手段。
- 没有密码就没有信息安
- 什么是信息安全？
  - 信息安全、网络安全、
    全、计算机信息安全、
  - 属性：机密性、完整性、
- 习近平指出：没有网络
- 2015.6.11“网络空间安全”国家一级学科获批……

2.2 区块链与密码学

- 区块链就是用信息安全的技术保障区块链网络、区块链数据的安全。
- 为了保证存储于区块链中的信息的安全与完整，区块及区块链的定义和构造中使用了包含哈希函数和椭圆曲线公钥密码技术在内的大量现代密码学技术。
- 同时这些密码学技术也被应用于设计基于工作量证明的共识算法并识别用户。
- 区块链代表了密码学与安全领域数十年来研究与突破的巅峰！来源于信息安全、反哺信息安全……

北方工业大学

「在区块链的江湖中，每个人都是骗子」

- 江湖多风波，舟楫恐失坠
- 人在江湖飘，哪能不挨刀

2.3 江湖多风波 - 江湖上流传的一口箱子

一个人，一口箱子。

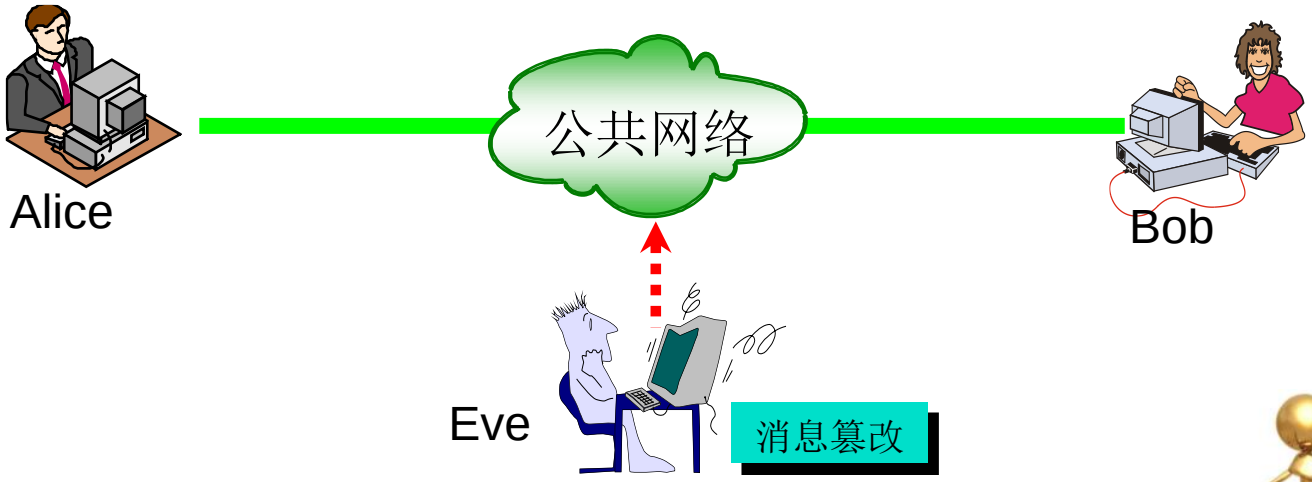
一个沉默平凡的人，提着一口陈旧平凡的箱子，在满天夕阳下，默然地走入了长安古城。

——古龙《英雄无泪》

2.3 江湖多风波 - 互联网 + 江湖的攻击 - 窃听

- 受威胁的属性：机密性
- 可应对的技术：加密

2.3 江湖多风波 - 互联网 + 江湖的攻击 - 篡改

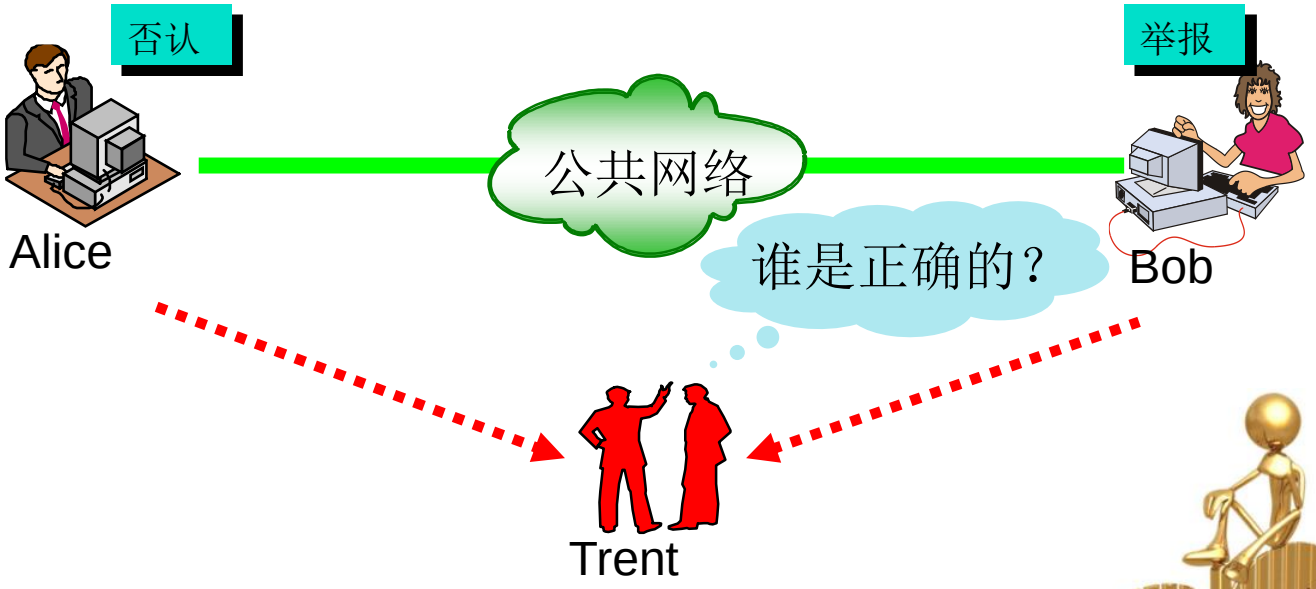


- 受威胁的属性：完整性
- 可应对的技术：哈希函数

2.3 江湖多风波 - 互联网 + 江湖的攻击 - 伪装

- 受威胁的属性：认证性
- 可应对的技术：消息认证（哈希函数）

2.3 江湖多风波 - 互联网 + 江湖的攻击 - 否认

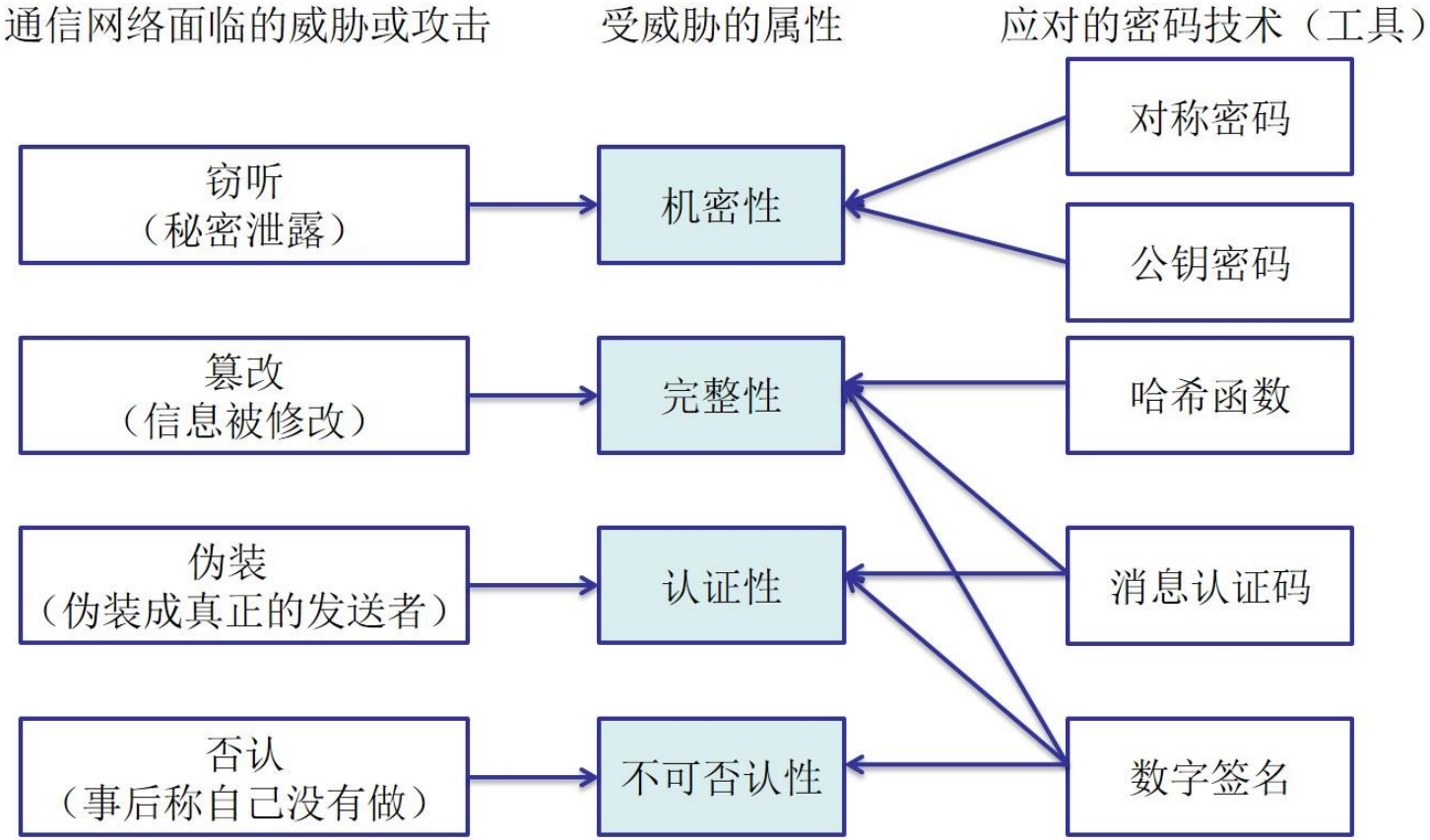


- 受威胁的属性：不可否认性
- 可应对的技术：数字签名

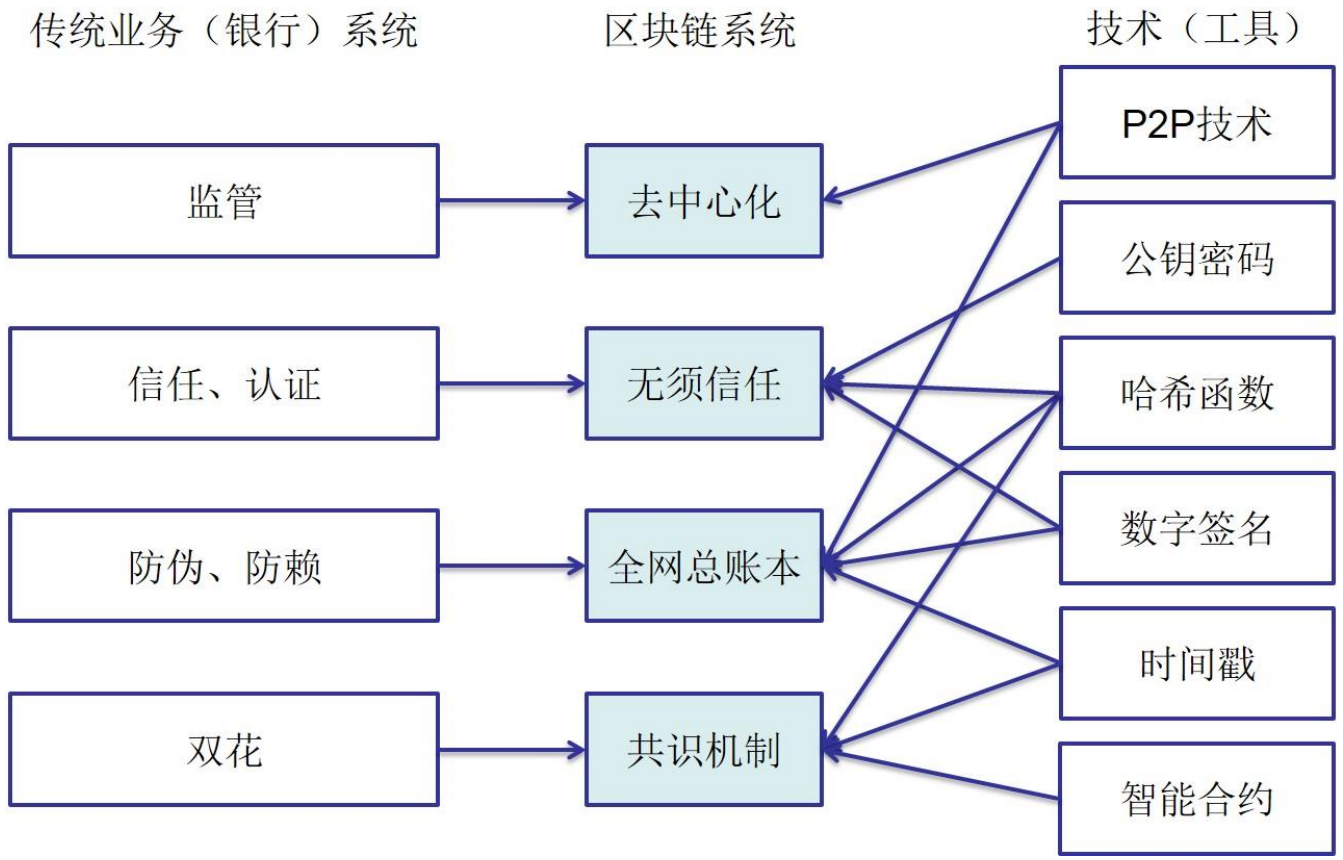
2.3 江湖多风波 - 密码学家的工具箱

- 对称密码
- 哈希函数（单向散列函数）
- 消息认证码
- 公钥密码
- 数字签名
- 伪随机数生成器

2.3 江湖多风波 - 密码学家的工具箱



2.3 江湖多风波 - 区块链江湖 - 安全工具箱



北方工业大学

Q&A

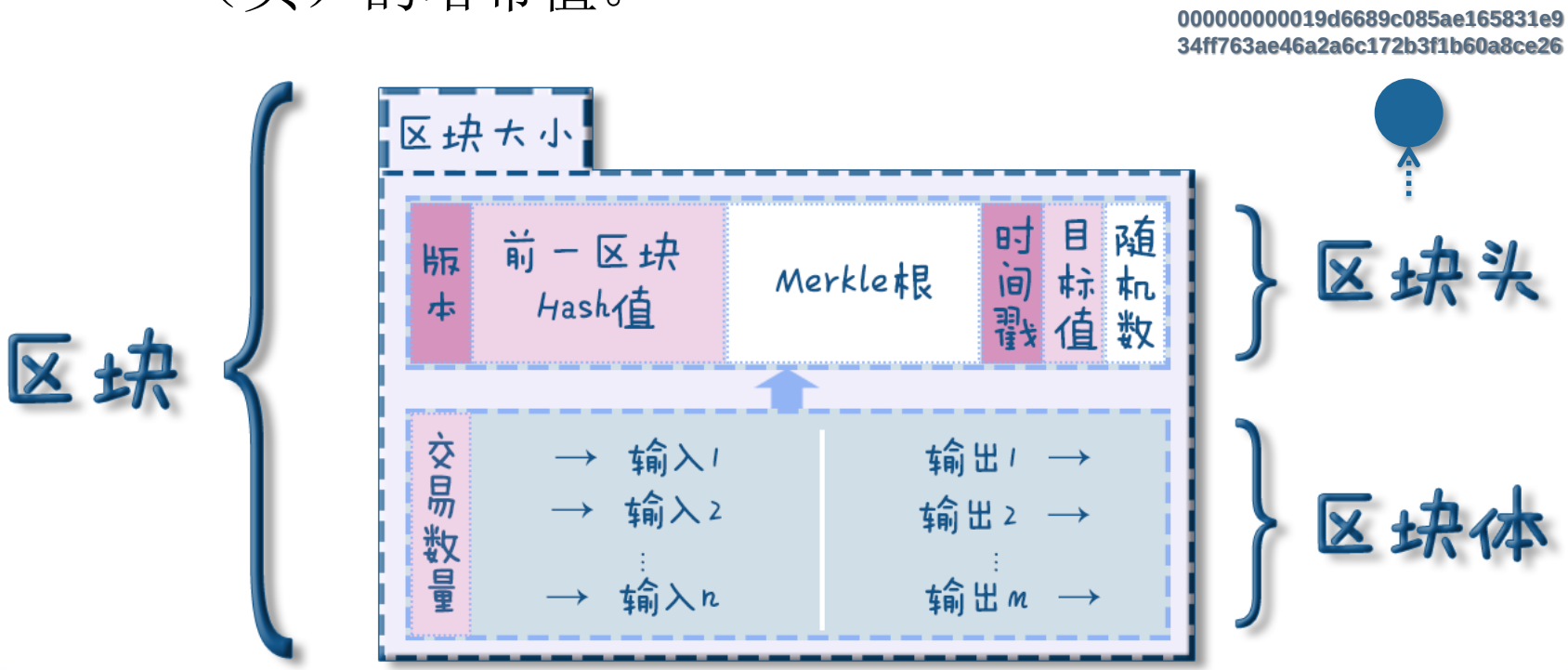
第一讲 区块链概述

本讲主要内容

- ✓ 构建诚信社会
- ✓ 区块链与密码学
- ➢ 区块链技术原理

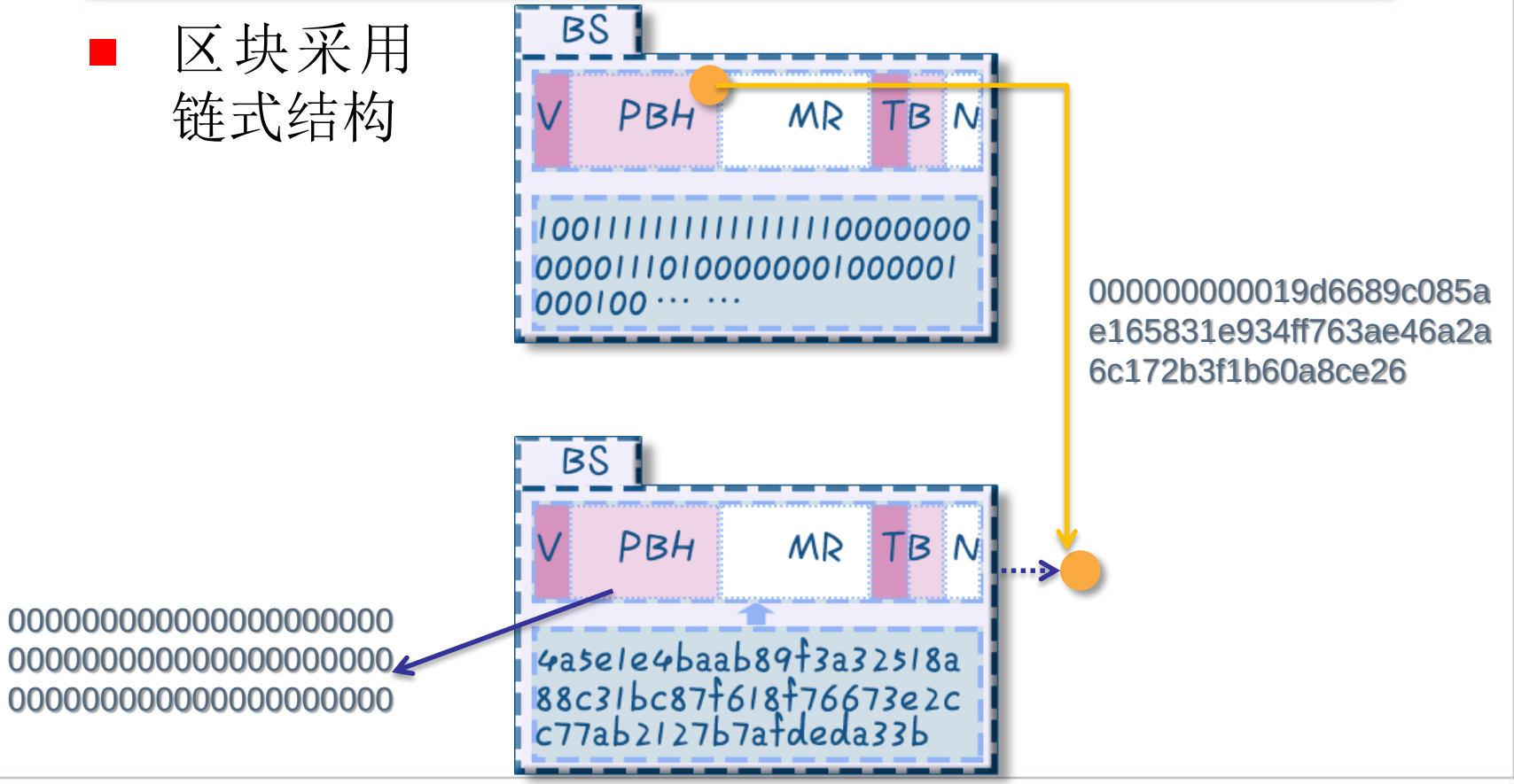
3.1 区块链技术原理 - 区块

- 区块链存储的基本单元是区块，区块的标识是区块（头）的哈希值。

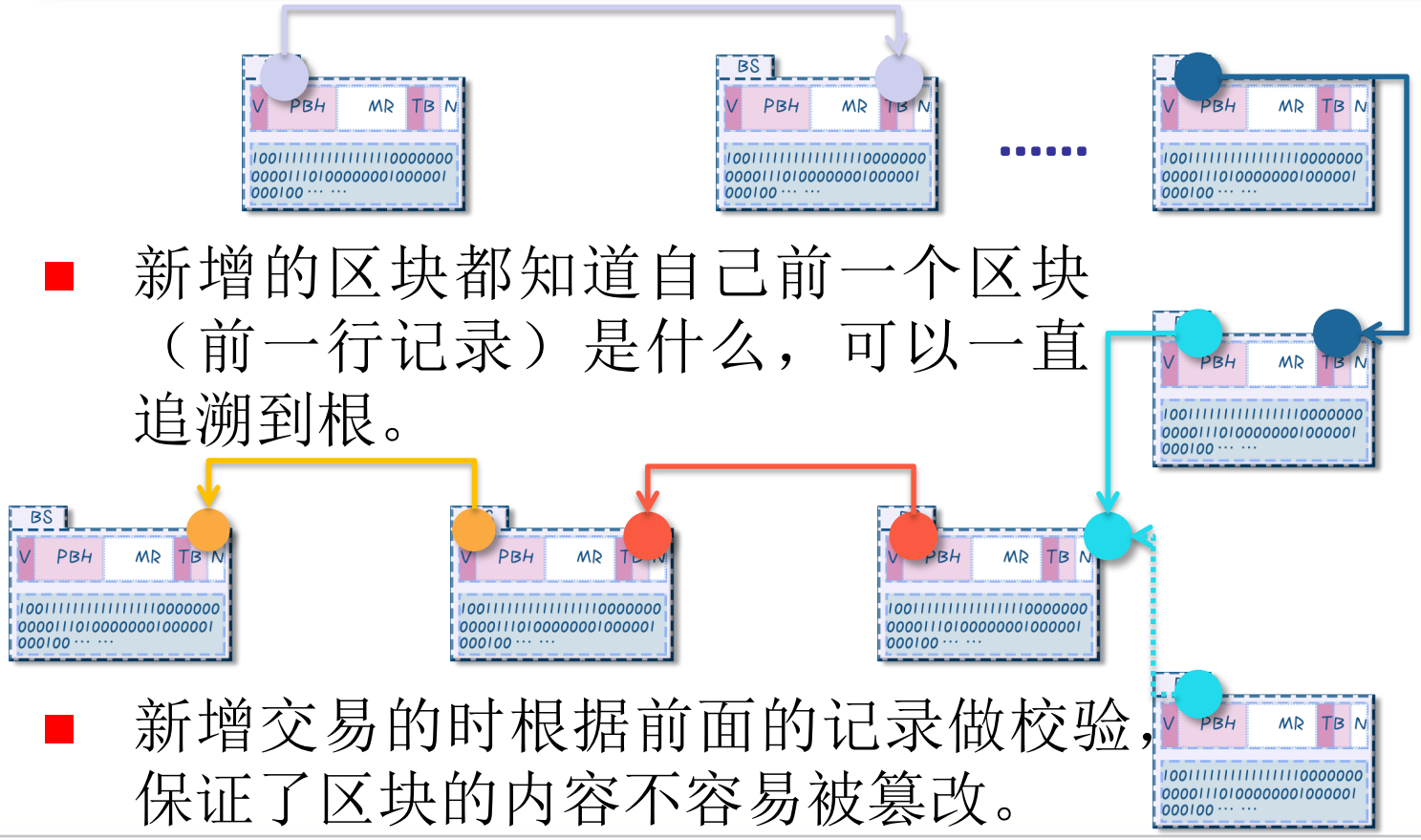


3.1 区块链技术原理 - 区块

- 区块采用链式结构



3.1 区块链技术原理 - 区块



- 新增的区块都知道自己前一个区块（前一行记录）是什么，可以一直追溯到根。
- 新增交易的时根据前面的记录做校验，保证了区块的内容不容易被篡改。

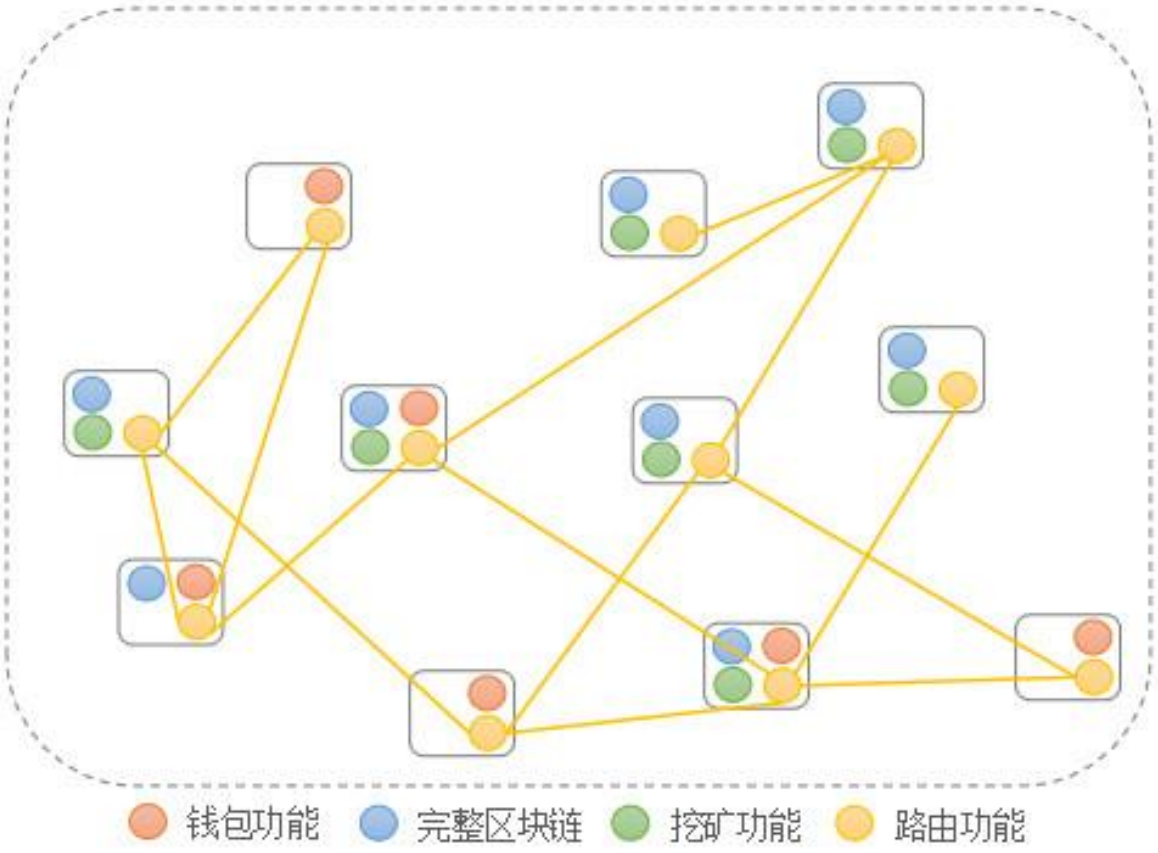
3.1 区块链技术原理 - 区块数据结构

- 比特币区块数据结构表
- 比特币区块数据结构思维导图（图片）
- 比特币区块链数据结构E-R图
- 比特币0.1.5源码及UML图

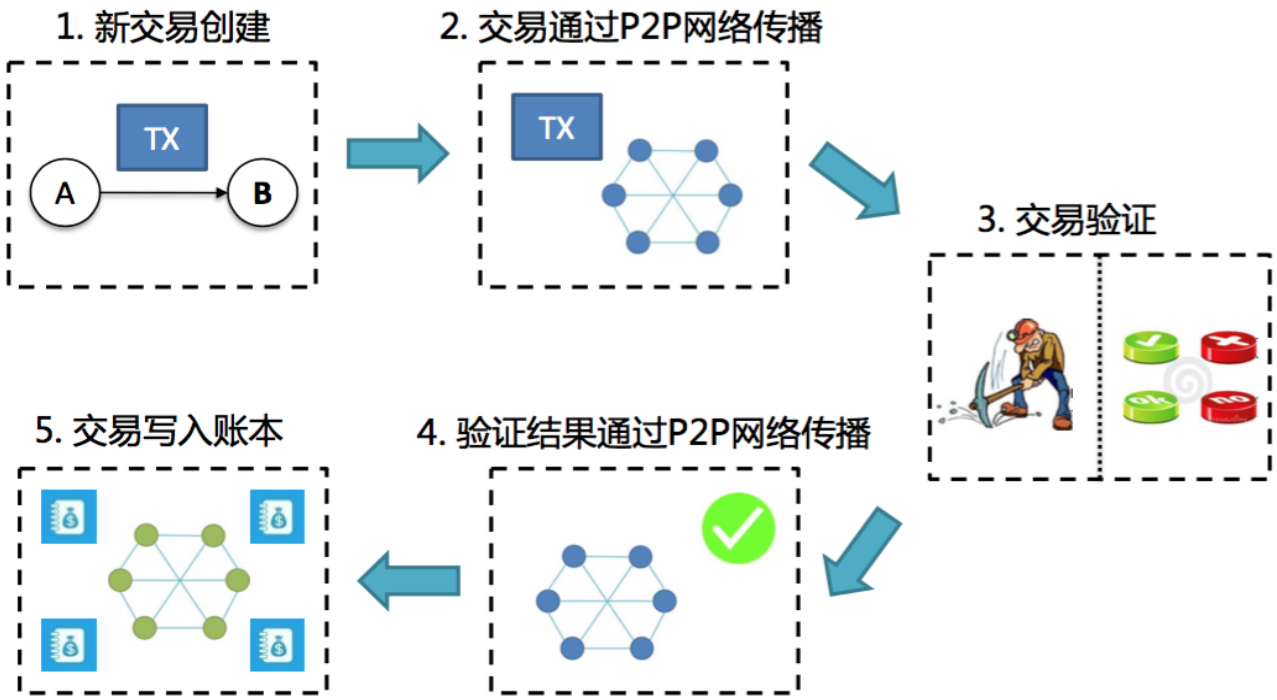
3.1 区块链技术原理 - 区块数据

version		01 00 00 00
input count		01
input	previous output hash (reversed)	48 4d 40 d4 5b 9e a0 d6 52 fc a8 25 8a b7 ca a4 25 41 eb 52 97 58 57 f9 6f b5 0c d7 32 c8 b4 81
	previous output index	00 00 00 00
	script length	8a
	scriptSig	47 30 44 02 20 2c b2 65 bf 10 70 7b f4 93 46 c3 51 5d d3 d1 6f c4 54 61 8c 58 ec 0a 0f f4 48 a6 76 c5 4f f7 13 02 20 6c 66 24 d7 62 a1 fc ef 46 18 28 4e ad 8f 08 67 8a c0 5b 13 c8 42 35 f1 65 4e 6a d1 68 23 3e 82 01 41 04 14 e3 01 b2 32 8f 17 44 2c 0b 83 10 d7 87 bf 3d 8a 40 4c fb d0 70 4f 13 5b 6a d4 b2 d3 ee 75 13 10 f9 81 92 6e 53 a6 e8 c3 9b d7 d3 fe fd 57 6c 54 3c ce 49 3c ba c0 63 88 f2 65 1d 1a ac bf cd
	sequence	ff ff ff ff
output count		01
output	value	62 64 01 00 00 00 00 00
	script length	19
	scriptPubKey	76 a9 14 c8 e9 09 96 c7 c6 08 0e e0 62 84 60 0c 68 4e d9 04 d1 4c 5c 88 ac
block lock time		00 00 00 00

3.2 区块链技术原理 - 节点网络

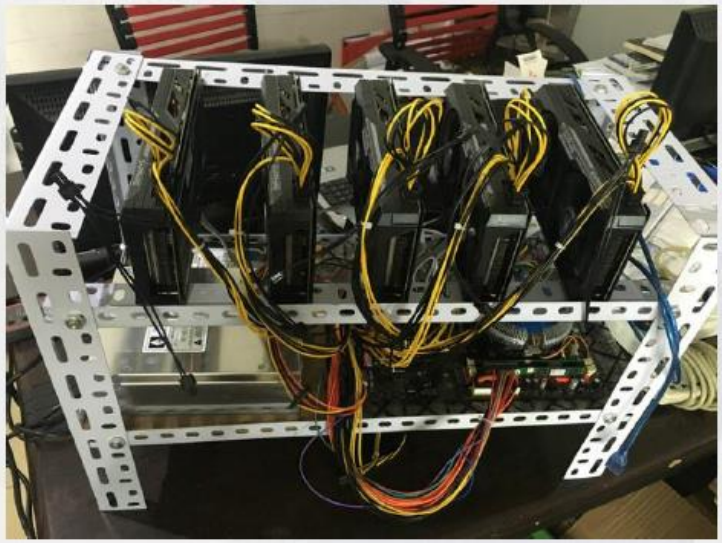


3.3 区块链技术原理 - 交易过程



3.3 区块链技术原理 - 挖矿

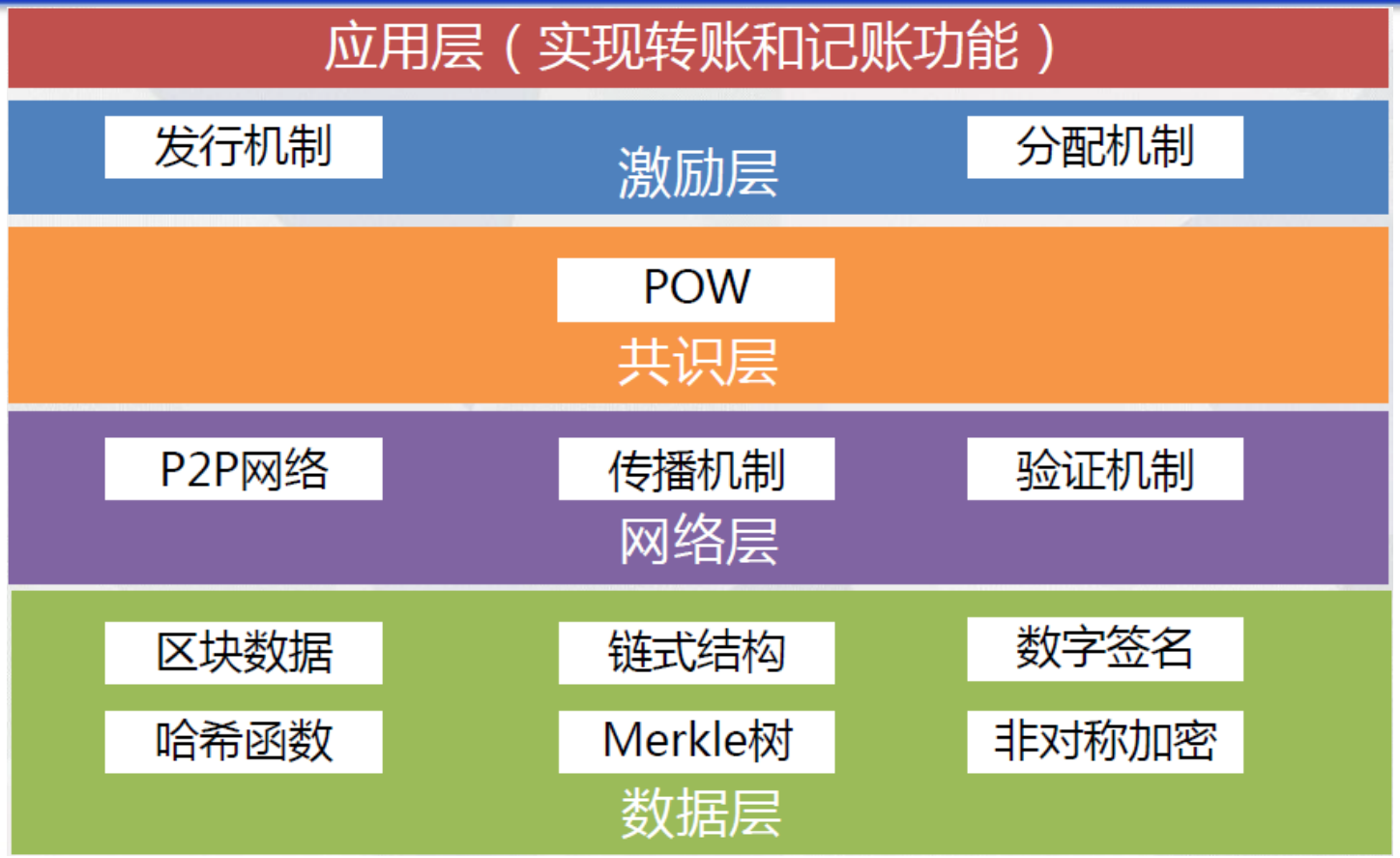
CPU挖矿 → 显卡挖矿 → 专用芯片矿机 → 矿池



第一讲 区块链概述


挖矿原理示意图
固定
固定
可变
改变收录交易数量、顺序、Coinbase
可变
固定范围
固定
调节算法明确，全网一致
可变
四个字节
nVersion
hashPrevBlock
hashMerkleRoot
nTime
nBits
nNonce
Hash函数
版本号
前一个区块Hash
交易Merkle树根
时间戳
难度
随机数
连续0的个数为 n
该值要小于当前区块难度目标值m
00000...011010111...11001
总长度为256位
挖到块的条件是前n个比特位全部为0，n越大，难度越大
假设最低难度对应最大目标值为M，区块难度为：M/m

3.3 区块链技术原理 - 基础技术架构



第一讲 区块链概述

本讲主要内容

- ✓ 构建诚信社会
- ✓ 区块链与密码学
- ✓ 区块链技术原理

作业

- C++面向对象思想—编程实现
  - 封装
  - 继承
  - 多态
- 下载比特币源码BitCoin v0.01或v0.1.5
- SourceInsight、UltraEdit、DevC++、VS2013

北方工业大学

Thank You !